REMARKS

Reconsideration and allowance are requested.

Applicants appreciate the consideration of the documents submitted in the various information disclosure statements. The Examiner indicates that another copy of the UK search report dated April 28, 2004 is needed, and one is supplied with this response. In addition, the Examiner is requested to initial the Other Documents entry entitled, "Trusted Computing Group...," listed on the FB-A820 form submitted with the information disclosure statement filed on June 2, 2004.

The office action did not acknowledge the foreign priority claims and receipt of the certified copies of the priority documents filed on April 20, 2004. Such acknowledgement is requested.

Most of the claims stand rejected for anticipation based on Letwin EP 0 574 032 A1. This rejection is respectfully traversed.

To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. *Scripps Clinic & Research Found. v. Genentec, Inc.*, 927 F.2d 1565 (Fed. Cir. 1991). Every limitation contained in the claims must be present in the reference, and if even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Letwin fails to satisfy this rigorous standard.

Letwin discloses a method and operating system for executing programs in a multi-mode microprocessor. The problem addressed by Letwin is a compatibility problem arising due to differences between the Intel 8086 and 80286 microprocessors architectures (see the background text and column 4, lines 37 to 44). In the real mode, the 80286 microprocessor architecture emulates the 8086 microprocessor architecture, in the protected mode, the 80286 runs natively. So the two processor modes exist in order to provide backward compatibility with an earlier generation of microprocessor architecture. Letwin is not focused on the security problems to which the claims in this application are directed.

The Examiner equates the non-secure mode" of claim 1 with the real mode in Letwin and the "secure mode" of claim 1 with the "protected mode" of Letwin. But the Examiner fails to identify where Letwin describes the "plurality of domains" or the "secure domain" and "non-secure domain" recited in claim 1. In fact, Letwin fails to teach *both* secure and non-secure modes *and* secure and non-secure domains.

Claim 1 also recites "said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode." For this feature, the Examiner points to column 4, lines 17 to 36 of Letwin. But Letwin fails to meet the strict secure data access demarcation recited in the claim. In column 2, lines 23 to 26, Letwin states that the "real mode" is limited to one megabyte of accessible physical memory. But then in column 4, lines 25 to 36, Letwin allows the processor in the real mode to address memory locations both above one megabyte (column 4, lines 28 to 29) and below one megabyte (column 4, lines 31 to 33).

For the same reasons, Letwin is deficient with respect to the claim recitation: "a memory configured to store data required by the processor and comprising secure memory for storing secure data and non-secure memory for storing non-secure data." The "protected mode" memory in Letwin is nevertheless accessible in the real mode, which means the "protected mode" memory is not secure memory. Secure data stored in the "protected mode" memory can be accessed in the real mode, which the Examiner equates with the claimed non-secure mode.

The memory in claim 1 contains "a non-secure table and a secure table, the non-secure table being within the non-secure memory and ... the secure table being within the secure memory." The Examiner points to column 4, lines 5 to 16 and Figure 3 for this recitation. Here, Letwin discloses "protected mode descriptor tables to produce a resulting base address identical to that obtained in real mode" (column 4, line 10 to 12), but Letwin does not disclose a "non-secure table." The "descriptor table" in Letwin's Figure 3 is used to perform a mapping in the protected mode (column 10, lines 34-53), but it is not used for the real mode where memory addressing is performed in terms of physical or "real addresses" (column 10, lines 6-9). In the real mode, the segment selector and offset are combined as shown in Figure 1 to produce the 20-bit physical address (column 10, lines 17-19).

Consequently, Letwin also fails to disclose a "non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor." For this feature, the Examiner relies on column 9, line 51 to column 10, line 53. Here, Letwin's description of "real mode" addressing (column 10, lines 6 to 33) does not refer to tables or descriptors. Letwin describes "descriptor tables" only in the context of "protected mode" addressing (column 10, line 34, to column 11, line 12). So Letwin lacks the claimed non-secure table.

Claim 1 further recites "the internal storage unit comprising a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table." Even though Letwin lacks the claimed non-secure table, the Examiner points to column 7, lines 6 to 27 as supposedly teaching the "flag associated with each descriptor stored feature." Applicants disagree. This portion of Letwin simply discloses that *a program* written for the microprocessor *includes a flag* indicating whether the program is designed to run in real mode or protected mode, i.e., in the native 80286 architecture or in the emulated 8086 architecture. A flag which determines where the program is stored in main memory cannot be reasonably equated with "an internal storage unit" of the "memory management unit" "comprising a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table," particularly since Letwin lacks a non-secure table.

Letwin further fails to disclose the claim feature of performing "the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table." Letwin's descriptor tables for use in the "protected mode" are used for mapping virtual addresses (column 10, lines 40 to 43). There is no disclosure in Letwin of deriving "access control information" from the descriptors stored in the table.

Lacking multiple features recited in independent claim 1 and analogous method claim features in independent claim 13, the anticipation rejection based on Letwin must be withdrawn. Ellison fails to remedy the deficiencies of Letwin. Accordingly, the prior art rejections should be withdrawn.

The application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: ______________________
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100